THE LAW OFFICES OF
EDMOND A. DEFRANK

20145 VIA MEDICI
NORTHRIDGE, CALIFORNIA 91326

INTELLECTUAL PROPERTY
LAW INCLUDING PATENTS,
TRADEMARKS AND COPYRIGHTS

TELEPHONE: (818) 885-1575
FACSIMILE: (818) 885-5750

TO: USPTO/ Examiner C. Shin Hon, Group 2131

FAX: (703) 872-9306

TEL: (703) 305-8654

FROM: Edmond DeFrank

DATE: February 28, 2005

RE: **APPEAL BRIEF TO THE BOARD OF PATENT APPEALS**
Serial No. 09/641,929
Our Docket No. 10001687-1
Entitled: **ASSURED PRINTING OF DOCUMENTS OF VALUE**
Filed: August 17, 2000
By: Kevin G. Currans.

Pages: 50 (NOT including cover sheet)

Please find attached an Appeal Brief for the above matter. Also included is a Transmittal Letter.

Thank you.

Edmond A. DeFrank

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10001687-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Kevin G. Currans	Confirmation No.:	6418
Application No.:	09/641,929	Examiner:	C. Shin Hon
Filing Date:	Aug. 17, 2000	Group Art Unit:	2131
Title:	ASSURED PRINTING OF DOCUMENTS OF VALUE		

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on Dec. 30, 2004.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $500.00. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit:_____

OR

(X) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (703) 872-9306 on Feb. 28, 2005

Number of pages: 50

Typed Name: Edmond A. DeFrank

Signature: Edmond A. DeFrank

Respectfully submitted,

Kevin G. Currans

By Edmond A. DeFrank

Edmond A. DeFrank
Attorney/Agent for Applicant(s)
Reg. No. 37,814

Date: Feb. 28, 2005

Telephone No.: (818) 885-1575

Rev 12/04 (Apbrief)

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10001687-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Kevin G. Currans

Confirmation No.: 6418

Application No.: 09/641,929

Examiner: C. Shin Hon

Filing Date: Aug. 17, 2000

Group Art Unit: 2131

Title: ASSURED PRINTING OF DOCUMENTS OF VALUE

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on Dec. 30, 2004.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $500.00. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit:_____

OR

(X) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (703) 872-9306 on Feb. 28, 2005

Number of pages: 50

Typed Name: Edmond A. DeFrank

Signature: Edmond A. DeFrank

Respectfully submitted,

Kevin G. Currans

By Edmond A. DeFrank

Edmond A. DeFrank

Attorney/Agent for Applicant(s)
Reg. No. 37,814

Date: Feb. 28, 2005

Telephone No.: (818) 885-1575

Rev 12/04 (Apbnef)

RECEIVED
CENTRAL FAX CENTER

FEB 2 8 2005

Attorney Docket No: 10001687-1 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of Kevin G. Currans	Group Art Unit: 2131
Entitled: **ASSURED PRINTING OF DOCUMENTS OF VALUE**	Examiner: C. Shin Hon
Serial No.: 09/641,929	
Filing Date: August 17, 2000	

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, LP.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to the assignee which will directly affect or be directly affected by or have a bearing on the Board's decision pending the appeal.

III. STATUS OF CLAIMS

Claim 5 has been cancelled and claims 1-4 and 6-23 stand rejected. Thus, the

Appellants file the present Appeal Brief in response to the Examiner's rejection of claims 1-4 and 6-23 in a Final Office Action dated September 2, 2004. Claims 1-4 and 6-23 represent all of the remaining claims from the originally filed application. The Appellants respectfully appeal the Examiner's final rejection of Claims 1-4 and 6-23.

IV. STATUS OF AMENDMENTS

An amendment under 37 CFR 1.116 was filed on November 2, 2004 in response to the Final Office Action dated September 2, 2004. In this amendment, minor non-substantive amendments were made to claims 1 and 4. In response, the Examiner sent an Advisory Action dated December 15, 2004 and checked the box on the Advisory Action form (PTOL-303) stating that the proposed amendment would not be entered, without providing any additional explanation. As such, claims 1-4 and 6-23 remain as presented in the May 27, 2004 amendment.

V. SUMMARY OF THE INVENTION

The present invention provides a method and apparatus for controlling printing of a document delivered via a computer network. In general, a first portion of a document is encrypted using at least a first encryption key, thereby creating a partially encrypted file. The partially encrypted file is transmitted via the computer network. A second portion of the transmitted partially encrypted file is printed and at least a serialized print number is returned. In response, the first encryption key is received. The first portion of the partially encrypted file is then decrypted and printed. This allows verification that the document was printed from an electronic file that was transmitted to and printed from a remote print mechanism and enables a document or file distributor to control re-distribution by conclusively determining whether a document printed from a file was printed in whole or in part.

In particular, the process includes the steps of encrypting a document and or parts thereof that is to be transferred electronically, transmitting the encrypted document to an intended party via a data network, such as the Internet, partially decrypting the document using a first decryption key so as to enable the document to be verified that it was properly received, and printing part of the document up to a point at which a second decryption key

is required. If the document is successfully printed down to the point where a second encryption key is required, the recipient of the document returns to the sender, an indicia, such a serial number of the document, which has been physically printed on the document at the time, that the document had started to print successfully. Receipt of the partial-printing proof by the document sender triggers the transmission to the document recipient (i.e., the printer and not the user's browser), the second decryption key by which the remaining portion of the document can be decrypted and printed by the recipient (i.e., the printer and not the user's browser).

Receipt of the indicia that the document was at least partially printed is created by the recipient's printer or print mechanism using a "Serialized Print." Upon the document sender's receipt of the indicia that the document was at least partially printed, the document recipient will thereby have provided to the document sender, conclusive proof that the entire document was received successfully as a "Guaranteed Print." The accuracy of the document that was printed can be determined and numerical indicia of output print quality can be generated such that a document sender provided with the print quality indicia can know whether the document that was printed was in fact a reasonably facsimile of the document that was electronically sent. Using the indicia of printing that was received by the sender, as well as an objective indicia of the output print quality documents that are sent electronically but which do not reasonable resemble their original condition as sent by the sender can be selectively retransmitted by the document sender at the document sender's discretion.

VI. ISSUES

Patentability of Claims 1-4 and 6-23

Whether claims 1, 2, 4, 6, 7, 10, 20, 21 and 23 are unpatentable under 35 U.S.C. § 103(a) over six (6) references including Christensen et al. (U.S. Publication No. US2002/0071559) in view of Nunley et al. (U.S. Patent No. 4,404,649) and further in view of Blumenthal et al. (U.S. Patent No. 5,784,460) and further in view of Wiegley (U.S. Patent No. 6,711,677) and further in view of Sansone (U.S. Patent No. 6,373,587) and further in view of Nishikawa (U.S. Pub. No. 20020048039).

Whether claims 3 and 22 are unpatentable under 35 U.S.C. § 103(a) over seven (7) references including Christensen et al. in view of Nunley et al. and further in view of Blumenthal et al. and further in view of Wiegley and further in view of Sansone and further in view of Nishikawa and further in view of Chan et al. (U.S. Patent No. 6,378,070).

Whether claims 12, 13, 17 and 18 are patentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg et al. (U.S. Patent No. 6,363,357) and further in view of Wiegley and further in view of Sansone and further in view of Nishikawa (U.S. Pub. No. 20020048039).

Whether claim 14 is unpatentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg and further in view of Sansone. Whether claim 16 is unpatentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg and further in view of Sansone and further in view of Blumenthal et al.

VII. GROUPING OF CLAIMS

For each ground of rejection which appellant contests herein which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

VIII. ARGUMENTS

A. The Examiner's Rationale for the Rejection of Claims 1-4 and 6-23

On pages 2 through 6 of the Final Office Action dated September 2, 2004, the Examiner discussed numerous references, one at a time in rejecting the claims. During the discussion of each reference, first the Examiner compared a single element of the Appellant's claims to a single element of a main cited reference. Second, the Examiner admitted that a second element of the Appellant's claims was not disclosed by the main reference but stated that it would have been obvious to add a second element of a second cited reference. Next, the Examiner admitted that the main and second references lacked a third element of the Appellant's claims but stated that it would have been obvious to add a third element of a third cited reference to the main and second references. The

Examiner then admitted that the third, second and main references lacked a fourth element of the Appellant's claims but stated that it would have been obvious to add a fourth element of a fourth cited reference to the main, second and third references. The Examiner then admitted that the fourth, third, second and main references lacked a fifth element of the Appellant's claims but stated that it would have been obvious to add a fifth element of a fifth cited reference to the main, second, third and fourth references. The Examiner then admitted that the fifth, fourth, third, second and main references lacked a sixth element of the Appellant's claims but stated that it would have been obvious to add a sixth element of a sixth cited reference to the main, second, third, fourth and fifth references.

With regard to claims 1, 2, 4, 6, 7, 10, 11, 20, 21 and 23, the Examiner continued this piece-meal approach of "tacking-on" another element of another reference each time an element of the claims was not disclosed, taught or suggested in the previous reference until **six (6)** references were combined. With regard to claims 3 and 22, the Examiner continued this "tacking-on" approach until **seven (7)** references were combined.

B. The Appellant Submits that the Examiner's Rejections Were Improper.

1. The Examiner ignored limitations of the claims and mischaracterized the references, thus, the rejections should be withdrawn.

According to case law and the MPEP, all of the claimed elements of an Appellant's invention **must be considered**. (In re Kotzab, 55 USPQ 2d 1313, 1318 (Fed. Cir. 2000). *MPEP 2143.*) [*emphasis added*]. If **one** of the elements of the Appellant's invention is missing from or not taught in the cited references and the Appellant's invention has advantages not appreciated by the cited references, then no prima facie case of obviousness exists. (*MPEP 2143.03).* The Federal Circuit Court has stated that it was error not to distinguish claims over a combination of prior art references where a material limitation in the claimed system and its purpose was not taught therein. In Re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

The cited combined references do **not** disclose, teach or suggest the Appellant's claimed invention that includes decrypting at the printer a first portion of the partially

encrypted file, printing at least a second portion of the partially encrypted file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and printing at least a portion of the decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

In contrast, although the Examiner used Nunley et al. as a reference to show serialized printing, the Examiner mischaracterized Nunley. Namely, Nunley does **not** disclose, teach or suggest the Appellant's serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

Instead, Nunley et al. uses a pre written SICN on the original document to support data entry and **not** a unique serialized print number for the document file in the course of printing the document file, like the Appellant's claimed invention. Nunley et al. is using the SICN merely to produce a customer reference for getting data entry information for the record in question. Consequently, the Examiner mischaracterized Nunley et al., and thus, obviousness cannot be established by combining these references because Nunley et al. is missing elements of the Appellant's claim. ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). This **failure** of the combined cited references to disclose, suggest or teach all of the elements of the Appellant's claimed invention indicates a lack of a prima facie case of obviousness (*MPEP 2143*).

2. The Examiner ignored a teaching away, thus, the rejections should be withdrawn

Even though the combination of the **six or seven** cited references **does not** produce all of the elements of the claimed invention, these references **should not** even be considered together since there is no motivation to combine the cited references. It is well-

settled law that there **must be** a basis in the references for combining or modifying the references. C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 48 USPQ 2d 1225, (Fed. Cir. 1998).

Specifically, obviousness cannot be established because Christensen et al. **teaches away** from the claimed invention. This is because the computer in Christensen et al. first fully decrypts the document and then transmits the fully decrypted document to the printer, which teaches away from the Appellant's claimed performing decryption at the printer. In particular, Christensen et al. explicitly states in the Abstract that encrypted "...data is transmitted from a first computer to a second computer, and the decryption key has to be requested each time the user want to gain access to the data in an unencrypted form." Moreover, Christensen et al. continues to state in parapgraph [0022] that "...(i.e. after K.sub.d has been used to decrypt the encrypted data) K.sub.d must be rendered unfit for use. This must be done in order to prevent the user from gaining access to K.sub.d. That is, K.sub.d may only be obtained and used temporarily, and the user may not at any time gain direct access to K.sub.d."

As a result, modifying the decryption location in Christensen et al. would modify the entire system in Christensen et al. and render the system being modified unsatisfactory for its intended purpose. Hence, the main function of Christensen et al. would be destroyed because the system in Christensen et al. specifically requires decryption at the computer. For example, if decryption were moved, an unscrupulous user would be able to modify the printer driver, for example, by changing the printer driver name. In this case, the unscrupulous user would be able to electronically capture the print job and redistribute it easily. In many cases, printer drivers are represented and differentiated by their device context, which is stored in the registry, and can easily be shared via a registry file.

As required by the case law and the MPEP, "[I]f proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). MPEP 2143.01. Therefore, the proposed modification is **not** proper and one of ordinary skill in the art would not find a reason to make the proposed modification. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

As such, this "teaching away" cannot be ignored. As such, obviousness cannot be established by combining these references. W.L. Gore& Assocs. V. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983).

3. The Examiner used improper hindsight to reject the claims, thus, the rejections should be withdrawn.

It is well-settled law that there must be a basis in the references for combining or modifying the references. Namely, the Examiner **cannot** use a "tack-on" approach to **arbitrarily "pick and choose" elements** from numerous references and combine these elements using hindsight. Any combination of elements in a manner that reconstructs the Appellant's invention only with the benefit of **hindsight** is insufficient to present a prima facie case of obviousness. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 230 USPQ 416 (Fed. Cir. 1986). [*emphasis added*].

Evidence that the Examiner used hindsight is clearly confirmed by the fact that the Examiner cited six (6) references for a single rejection and seven (7) references for another single rejection without providing any reasoning for combining these references. Contrary to the Examiner's approach, the Appellant submits that there must be some reason, suggestion, or motivation found in the references whereby a person of ordinary skill in the field of the invention would make the combination. **That knowledge cannot come from the applicant's invention itself.** In re Oetiker, 977 F.2d 1443, 24 USPQ 2d 1443, 1446 (Fed. Cir. 1992) [*emphasis added*].

Further, "[T]he genius of invention is often a combination of known elements which in hindsight seems preordained. To prevent hindsight invalidation of patent claims, the law requires some 'teaching, suggestion or reason' to combine cited references." Gambro Lundia AB v. Baxter Healthcare Corp., 110 F.3d 1573, 1579, 42 USPQ 2d 1378, 1383 (Fed. Cir. 1997). When the reference in question seems relatively similar "...**the opportunity to judge by hindsight is particularly tempting**. Consequently, the tests of whether to combine references need to be applied rigorously," especially when the Examiner uses numerous references. McGinley v. Franklin Sports Inc., 60 USPQ 2d 1001, 1008 (Fed. Cir. 2001). [*emphasis added*]. Since the Examiner's rejection is

unquestionably based on hindsight, the rejection is improper and must be withdrawn. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.

IX. CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-4 and 6-23 was erroneous, and reversal of the Examiner's decision is respectfully requested. Accordingly, the Appellants submit that all pending claims (claims 1-4 and 6-23) in the current case should be allowed.

Respectfully submitted,

Dated: February 28, 2005

Edmond A. DeFrank
Reg. No. 37,814
Attorney for Appellants

EDMOND A. DEFRANK
Attorney at Law
20145 Via Medici
Northridge, CA 91326
(818) 885-1575 TEL
(818) 885-5750 FAX

X. APPEAL BRIEF APPENDIX

The following represents claims 1-4 and 6-23 that are involved in the appeal of the above-identified application and are provided in accordance with the requirements of 37 CFR 1.192(c)(7). Claim 5 is not presented below because it was cancelled in a May 27, 2004 amendment:

1. A method to control printing of a document file delivered via a computer network comprising the steps of:

at a first computer:

encrypting at least a first portion of a document file using at least a first encryption key thereby creating a partially encrypted file;

transmitting the partially encrypted file to a second computer via said computer network;

at said second computer:

printing at least a second portion of said partially encrypted file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file;

returning to said first computer at least the serialized print number, and receiving, in response thereto, said first encryption key;

decrypting at the printer said first portion of said partially encrypted file to create a partially decrypted document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

2. A method in accordance with the method of claim 1 wherein said step of returning further comprises the step of providing payment.

3. A method in accordance with the method of claim 1 further including steps of:

before transmitting the partially encrypted file to a second computer, encrypting at least part of said partially encrypted file to form a twice-encrypted file using a second encryption key; and

prior to printing at least a second portion of said partially decrypted file, decrypting said twice-encrypted file using at least one of either said second encryption key or a third encryption key.

4. A method in accordance with the method of claim 1 wherein said serialized print methodology includes the steps of:

generating by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device;

returning said number to said first computer thereby enabling said second computer to receive said first key.

5. (canceled).

6. A system for controlling the printing of a document file delivered via a computer network comprising:

a first computer that encrypts at least a first portion of a document file using a first key;

a data transfer device coupled said first computer capable of transferring the partially encrypted document file to a second computer;

a print mechanism operatively coupled to said data transfer device, said print mechanism capable of receiving said document file and decrypting at least a portion of said first portion of said document file and printing said first portion using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

7. The system of claim 6 wherein said print mechanism is comprised of a computer operatively coupled to a printer.

8. The system of claim 6 wherein said print mechanism is comprised of a printer capable of generating serialized output.

9. The system of claim 6 wherein said print mechanism is comprised of a printer capable of guaranteeing output print quality.

10. Apparatus for controlling the printing of a document file delivered via a computer network, comprising:

a first computer coupled to a data transfer mechanism, said first computer capable of receiving via said data transfer mechanism, at least one partially encrypted document file from a second computer;

a print mechanism operatively coupled to said first computer, said print mechanism being capable of decrypting at least a portion of the encrypted file and printing at least a portion of said partially encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

11. Apparatus for controlling the printing of a document file delivered via a computer network comprising:

a first computer coupled to an Internet connection, said first computer capable of receiving data from a remote printer via said Internet connection, at least one partially encrypted document file from a second computer;

a networked print mechanism operatively coupled to said first computer via the Internet, said print mechanism being capable of decrypting at least a portion of the encrypted file and printing at least a portion of said partially encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending via the Internet the first computer information about the number of printed pages and output print quality of the document file.

12. A method of controlling the printing of a document delivered via a computer network comprising the steps of:

printing a first portion of the document with a remote printer, said first portion being unencrypted;

communicating, via the computer network, with an entity associated with the document to arrange for the printing of a remaining portion of the document;

receiving, as a result of said communicating step, an encrypted remaining portion of the document;

using the printer to decrypt said remaining portion;

printing said decrypted remaining portion using a guaranteed print methodology that includes sending information about the number of printed pages and output print quality of the document file; and

using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file.

13. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of providing payment to said entity.

14. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of ascertaining quality of said printed first portion.

15. A method in accordance with the method of claim 12 further comprises the step of generating a number correlating said document to a printing device printing said first portion.

16. A method in accordance with the method of claim 15 wherein said step of communicating further comprises the step of communicating said generated number.

17. A method of controlling the printing of a document delivered via a computer network to a user, comprising of the steps of:

encrypting a portion of the document;

transmitting an unencrypted portion of the document via the computer network to the user for printing;

receiving a communication related to a reception of said unencrypted portion by the user;

transmitting said encrypted portion of the document to the user via the computer network in response to said receiving step;

using a printer to decrypt at least a portion of the encrypted file and printing at least a portion of said encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

18. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a payment for the document.

19. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a proof that said unencrypted portion of the document was satisfactorily printed.

20. A method of controlling the printing of a partially encrypted document file delivered via a computer network, at least a first portion of which partially encrypted document is encrypted using at least a first encryption key, comprising the steps of:

printing using a printer at least a second portion of the partially encrypted document file;

creating a serialized print number that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and returning the serialized print number via the computer network;

receiving the first encryption key;

using the printer to decrypt the first portion to create a decrypted document file; and

printing said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

21. A method in accordance with the method of claim 20 further comprising the step of providing payment for the partially encrypted document.

22. A method in accordance with the method of claim 20 wherein at least part of the partially encrypted document file is further encrypted to form a twice-encrypted file using a second encryption key, further comprising the step of prior to printing at least a second portion of said partially decrypted document file, decrypting said twice-encrypted file using at least said second encryption key.

23. A method in accordance with the method of claim 21 wherein said step of creating a serialized print number further comprises the step of generating, by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device.

CERTIFICATE OF TRANSMISSION
I hereby certify that this paper and every paper referred to therein as being facsimile transmitted to: (703) 872-9319 of the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on February 28, 2005 (Date of Deposit) No. of Pages 50

EDMOND A. DEFRANK
By

Signature

Attorney Docket No: 10001687-1 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of Kevin G. Currans	Group Art Unit: 2131
Entitled: **ASSURED PRINTING OF DOCUMENTS OF VALUE**	Examiner: C. Shin Hon
Serial No.: 09/641,929	
Filing Date: August 17, 2000	

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, LP.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to the assignee which will directly affect or be directly affected by or have a bearing on the Board's decision pending the appeal.

III. STATUS OF CLAIMS

Claim 5 has been cancelled and claims 1-4 and 6-23 stand rejected. Thus, the

Appellants file the present Appeal Brief in response to the Examiner's rejection of claims 1-4 and 6-23 in a Final Office Action dated September 2, 2004. Claims 1-4 and 6-23 represent all of the remaining claims from the originally filed application. The Appellants respectfully appeal the Examiner's final rejection of Claims 1-4 and 6-23.

IV. STATUS OF AMENDMENTS

An amendment under 37 CFR 1.116 was filed on November 2, 2004 in response to the Final Office Action dated September 2, 2004. In this amendment, minor non-substantive amendments were made to claims 1 and 4. In response, the Examiner sent an Advisory Action dated December 15, 2004 and checked the box on the Advisory Action form (PTOL-303) stating that the proposed amendment would not be entered, without providing any additional explanation. As such, claims 1-4 and 6-23 remain as presented in the May 27, 2004 amendment.

V. SUMMARY OF THE INVENTION

The present invention provides a method and apparatus for controlling printing of a document delivered via a computer network. In general, a first portion of a document is encrypted using at least a first encryption key, thereby creating a partially encrypted file. The partially encrypted file is transmitted via the computer network. A second portion of the transmitted partially encrypted file is printed and at least a serialized print number is returned. In response, the first encryption key is received. The first portion of the partially encrypted file is then decrypted and printed. This allows verification that the document was printed from an electronic file that was transmitted to and printed from a remote print mechanism and enables a document or file distributor to control re-distribution by conclusively determining whether a document printed from a file was printed in whole or in part.

In particular, the process includes the steps of encrypting a document and or parts thereof that is to be transferred electronically, transmitting the encrypted document to an intended party via a data network, such as the Internet, partially decrypting the document using a first decryption key so as to enable the document to be verified that it was properly received, and printing part of the document up to a point at which a second decryption key

is required. If the document is successfully printed down to the point where a second encryption key is required, the recipient of the document returns to the sender, an indicia, such a serial number of the document, which has been physically printed on the document at the time, that the document had started to print successfully. Receipt of the partial-printing proof by the document sender triggers the transmission to the document recipient (i.e., the printer and not the user's browser), the second decryption key by which the remaining portion of the document can be decrypted and printed by the recipient (i.e., the printer and not the user's browser).

Receipt of the indicia that the document was at least partially printed is created by the recipient's printer or print mechanism using a "Serialized Print." Upon the document sender's receipt of the indicia that the document was at least partially printed, the document recipient will thereby have provided to the document sender, conclusive proof that the entire document was received successfully as a "Guaranteed Print." The accuracy of the document that was printed can be determined and numerical indicia of output print quality can be generated such that a document sender provided with the print quality indicia can know whether the document that was printed was in fact a reasonably facsimile of the document that was electronically sent. Using the indicia of printing that was received by the sender, as well as an objective indicia of the output print quality documents that are sent electronically but which do not reasonable resemble their original condition as sent by the sender can be selectively retransmitted by the document sender at the document sender's discretion.

VI. ISSUES

Patentability of Claims 1-4 and 6-23

Whether claims 1, 2, 4, 6, 7, 10, 20, 21 and 23 are unpatentable under 35 U.S.C. § 103(a) over six (6) references including Christensen et al. (U.S. Publication No. US2002/0071559) in view of Nunley et al. (U.S. Patent No. 4,404,649) and further in view of Blumenthal et al. (U.S. Patent No. 5,784,460) and further in view of Wiegley (U.S. Patent No. 6,711,677) and further in view of Sansone (U.S. Patent No. 6,373,587) and further in view of Nishikawa (U.S. Pub. No. 20020048039).

Whether claims 3 and 22 are unpatentable under 35 U.S.C. § 103(a) over seven (7) references including Christensen et al. in view of Nunley et al. and further in view of Blumenthal et al. and further in view of Wiegley and further in view of Sansone and further in view of Nishikawa and further in view of Chan et al. (U.S. Patent No. 6,378,070).

Whether claims 12, 13, 17 and 18 are patentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg et al. (U.S. Patent No. 6,363,357) and further in view of Wiegley and further in view of Sansone and further in view of Nishikawa (U.S. Pub. No. 20020048039).

Whether claim 14 is unpatentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg and further in view of Sansone. Whether claim 16 is unpatentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg and further in view of Sansone and further in view of Blumenthal et al.

VII. GROUPING OF CLAIMS

For each ground of rejection which appellant contests herein which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

VIII. ARGUMENTS

A. The Examiner's Rationale for the Rejection of Claims 1-4 and 6-23

On pages 2 through 6 of the Final Office Action dated September 2, 2004, the Examiner discussed numerous references, one at a time in rejecting the claims. During the discussion of each reference, first the Examiner compared a single element of the Appellant's claims to a single element of a main cited reference. Second, the Examiner admitted that a second element of the Appellant's claims was not disclosed by the main reference but stated that it would have been obvious to add a second element of a second cited reference. Next, the Examiner admitted that the main and second references lacked a third element of the Appellant's claims but stated that it would have been obvious to add a third element of a third cited reference to the main and second references. The

Examiner then admitted that the third, second and main references lacked a fourth element of the Appellant's claims but stated that it would have been obvious to add a fourth element of a fourth cited reference to the main, second and third references. The Examiner then admitted that the fourth, third, second and main references lacked a fifth element of the Appellant's claims but stated that it would have been obvious to add a fifth element of a fifth cited reference to the main, second, third and fourth references. The Examiner then admitted that the fifth, fourth, third, second and main references lacked a sixth element of the Appellant's claims but stated that it would have been obvious to add a sixth element of a sixth cited reference to the main, second, third, fourth and fifth references.

With regard to claims 1, 2, 4, 6, 7, 10, 11, 20, 21 and 23, the Examiner continued this piece-meal approach of "tacking-on" another element of another reference each time an element of the claims was not disclosed, taught or suggested in the previous reference until **six (6)** references were combined. With regard to claims 3 and 22, the Examiner continued this "tacking-on" approach until **seven (7)** references were combined.

B. The Appellant Submits that the Examiner's Rejections Were Improper.

1. The Examiner ignored limitations of the claims and mischaracterized the references, thus, the rejections should be withdrawn.

According to case law and the MPEP, all of the claimed elements of an Appellant's invention **must be considered**. (In re Kotzab, 55 USPQ 2d 1313, 1318 (Fed. Cir. 2000). *MPEP 2143.*) [*emphasis added*]. If **one** of the elements of the Appellant's invention is missing from or not taught in the cited references and the Appellant's invention has advantages not appreciated by the cited references, then no prima facie case of obviousness exists. (*MPEP 2143.03).* The Federal Circuit Court has stated that it was error not to distinguish claims over a combination of prior art references where a material limitation in the claimed system and its purpose was not taught therein. In Re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

The cited combined references do **not** disclose, teach or suggest the Appellant's claimed invention that includes decrypting at the printer a first portion of the partially

encrypted file, printing at least a second portion of the partially encrypted file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and printing at least a portion of the decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

In contrast, although the Examiner used Nunley et al. as a reference to show serialized printing, the Examiner mischaracterized Nunley. Namely, Nunley does **not** disclose, teach or suggest the Appellant's serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

Instead, Nunley et al. uses a pre written SICN on the original document to support data entry and **not** a unique serialized print number for the document file in the course of printing the document file, like the Appellant's claimed invention. Nunley et al. is using the SICN merely to produce a customer reference for getting data entry information for the record in question. Consequently, the Examiner mischaracterized Nunley et al., and thus, obviousness cannot be established by combining these references because Nunley et al. is missing elements of the Appellant's claim. ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). This **failure** of the combined cited references to disclose, suggest or teach all of the elements of the Appellant's claimed invention indicates a lack of a prima facie case of obviousness (*MPEP 2143*).

2. The Examiner ignored a teaching away, thus, the rejections should be withdrawn

Even though the combination of the **six or seven** cited references **does not** produce all of the elements of the claimed invention, these references **should not** even be considered together since there is no motivation to combine the cited references. It is well-

settled law that there **must be** a basis in the references for combining or modifying the references. C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 48 USPQ 2d 1225, (Fed. Cir. 1998).

Specifically, obviousness cannot be established because Christensen et al. **teaches away** from the claimed invention. This is because the computer in Christensen et al. first fully decrypts the document and then transmits the fully decrypted document to the printer, which teaches away from the Appellant's claimed performing decryption at the printer. In particular, Christensen et al. explicitly states in the Abstract that encrypted "...data is transmitted from a first computer to a second computer, and the decryption key has to be requested each time the user want to gain access to the data in an unencrypted form." Moreover, Christensen et al. continues to state in parapgraph [0022] that "...(i.e. after K.sub.d has been used to decrypt the encrypted data) K.sub.d must be rendered unfit for use. This must be done in order to prevent the user from gaining access to K.sub.d. That is, K.sub.d may only be obtained and used temporarily, and the user may not at any time gain direct access to K.sub.d."

As a result, modifying the decryption location in Christensen et al. would modify the entire system in Christensen et al. and render the system being modified unsatisfactory for its intended purpose. Hence, the main function of Christensen et al. would be destroyed because the system in Christensen et al. specifically requires decryption at the computer. For example, if decryption were moved, an unscrupulous user would be able to modify the printer driver, for example, by changing the printer driver name. In this case, the unscrupulous user would be able to electronically capture the print job and redistribute it easily. In many cases, printer drivers are represented and differentiated by their device context, which is stored in the registry, and can easily be shared via a registry file.

As required by the case law and the MPEP, "[I]f proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). MPEP 2143.01. Therefore, the proposed modification is **not** proper and one of ordinary skill in the art would not find a reason to make the proposed modification. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

As such, this "teaching away" cannot be ignored. As such, obviousness cannot be established by combining these references. W.L. Gore& Assocs. V. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983).

3. The Examiner used improper hindsight to reject the claims, thus, the rejections should be withdrawn.

It is well-settled law that there must be a basis in the references for combining or modifying the references. Namely, the Examiner **cannot** use a "tack-on" approach to **arbitrarily "pick and choose" elements** from numerous references and combine these elements using hindsight. Any combination of elements in a manner that reconstructs the Appellant's invention only with the benefit of **hindsight** is insufficient to present a prima facie case of obviousness. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 230 USPQ 416 (Fed. Cir. 1986). [*emphasis added*].

Evidence that the Examiner used hindsight is clearly confirmed by the fact that the Examiner cited six (6) references for a single rejection and seven (7) references for another single rejection without providing any reasoning for combining these references. Contrary to the Examiner's approach, the Appellant submits that there must be some reason, suggestion, or motivation found in the references whereby a person of ordinary skill in the field of the invention would make the combination. **That knowledge cannot come from the applicant's invention itself.** In re Oetiker, 977 F.2d 1443, 24 USPQ 2d 1443, 1446 (Fed. Cir. 1992) [*emphasis added*].

Further, "[T]he genius of invention is often a combination of known elements which in hindsight seems preordained. To prevent hindsight invalidation of patent claims, the law requires some 'teaching, suggestion or reason' to combine cited references." Gambro Lundia AB v. Baxter Healthcare Corp., 110 F.3d 1573, 1579, 42 USPQ 2d 1378, 1383 (Fed. Cir. 1997). When the reference in question seems relatively similar "...**the opportunity to judge by hindsight is particularly tempting**. Consequently, the tests of whether to combine references need to be applied rigorously," especially when the Examiner uses numerous references. McGinley v. Franklin Sports Inc., 60 USPQ 2d 1001, 1008 (Fed. Cir. 2001). [*emphasis added*]. Since the Examiner's rejection is

unquestionably based on hindsight, the rejection is improper and must be withdrawn. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.

IX. CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-4 and 6-23 was erroneous, and reversal of the Examiner's decision is respectfully requested. Accordingly, the Appellants submit that all pending claims (claims 1-4 and 6-23) in the current case should be allowed.

Respectfully submitted,

Dated: February 28, 2005

Edmond A. DeFrank
Reg. No. 37,814
Attorney for Appellants

EDMOND A. DEFRANK
Attorney at Law
20145 Via Medici
Northridge, CA 91326
(818) 885-1575 TEL
(818) 885-5750 FAX

X. APPEAL BRIEF APPENDIX

The following represents claims 1-4 and 6-23 that are involved in the appeal of the above-identified application and are provided in accordance with the requirements of 37 CFR 1.192(c)(7). Claim 5 is not presented below because it was cancelled in a May 27, 2004 amendment:

1. A method to control printing of a document file delivered via a computer network comprising the steps of:

at a first computer:

encrypting at least a first portion of a document file using at least a first encryption key thereby creating a partially encrypted file;

transmitting the partially encrypted file to a second computer via said computer network;

at said second computer:

printing at least a second portion of said partially encrypted file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file;

returning to said first computer at least the serialized print number, and receiving, in response thereto, said first encryption key;

decrypting at the printer said first portion of said partially encrypted file to create a partially decrypted document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

2. A method in accordance with the method of claim 1 wherein said step of returning further comprises the step of providing payment.

3. A method in accordance with the method of claim 1 further including steps of:

before transmitting the partially encrypted file to a second computer, encrypting at least part of said partially encrypted file to form a twice-encrypted file using a second encryption key; and

prior to printing at least a second portion of said partially decrypted file, decrypting said twice-encrypted file using at least one of either said second encryption key or a third encryption key.

4. A method in accordance with the method of claim 1 wherein said serialized print methodology includes the steps of:

generating by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device;

returning said number to said first computer thereby enabling said second computer to receive said first key.

5. (canceled).

6. A system for controlling the printing of a document file delivered via a computer network comprising:

a first computer that encrypts at least a first portion of a document file using a first key;

a data transfer device coupled said first computer capable of transferring the partially encrypted document file to a second computer;

a print mechanism operatively coupled to said data transfer device, said print mechanism capable of receiving said document file and decrypting at least a portion of said first portion of said document file and printing said first portion using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

7. The system of claim 6 wherein said print mechanism is comprised of a computer operatively coupled to a printer.

8. The system of claim 6 wherein said print mechanism is comprised of a printer capable of generating serialized output.

9. The system of claim 6 wherein said print mechanism is comprised of a printer capable of guaranteeing output print quality.

10. Apparatus for controlling the printing of a document file delivered via a computer network, comprising:

a first computer coupled to a data transfer mechanism, said first computer capable of receiving via said data transfer mechanism, at least one partially encrypted document file from a second computer;

a print mechanism operatively coupled to said first computer, said print mechanism being capable of decrypting at least a portion of the encrypted file and printing at least a portion of said partially encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

11. Apparatus for controlling the printing of a document file delivered via a computer network comprising:

a first computer coupled to an Internet connection, said first computer capable of receiving data from a remote printer via said Internet connection, at least one partially encrypted document file from a second computer;

a networked print mechanism operatively coupled to said first computer via the Internet, said print mechanism being capable of decrypting at least a portion of the encrypted file and printing at least a portion of said partially encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending via the Internet the first computer information about the number of printed pages and output print quality of the document file.

12. A method of controlling the printing of a document delivered via a computer network comprising the steps of:

printing a first portion of the document with a remote printer, said first portion being unencrypted;

communicating, via the computer network, with an entity associated with the document to arrange for the printing of a remaining portion of the document;

receiving, as a result of said communicating step, an encrypted remaining portion of the document;

using the printer to decrypt said remaining portion;

printing said decrypted remaining portion using a guaranteed print methodology that includes sending information about the number of printed pages and output print quality of the document file; and

using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file.

13. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of providing payment to said entity.

14. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of ascertaining quality of said printed first portion.

15. A method in accordance with the method of claim 12 further comprises the step of generating a number correlating said document to a printing device printing said first portion.

16. A method in accordance with the method of claim 15 wherein said step of communicating further comprises the step of communicating said generated number.

17. A method of controlling the printing of a document delivered via a computer network to a user, comprising of the steps of:

encrypting a portion of the document;

transmitting an unencrypted portion of the document via the computer network to the user for printing;

receiving a communication related to a reception of said unencrypted portion by the user;

transmitting said encrypted portion of the document to the user via the computer network in response to said receiving step;

using a printer to decrypt at least a portion of the encrypted file and printing at least a portion of said encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

18. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a payment for the document.

19. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a proof that said unencrypted portion of the document was satisfactorily printed.

20. A method of controlling the printing of a partially encrypted document file delivered via a computer network, at least a first portion of which partially encrypted document is encrypted using at least a first encryption key, comprising the steps of:

printing using a printer at least a second portion of the partially encrypted document file;

creating a serialized print number that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and returning the serialized print number via the computer network;

receiving the first encryption key;

using the printer to decrypt the first portion to create a decrypted document file; and

printing said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

21. A method in accordance with the method of claim 20 further comprising the step of providing payment for the partially encrypted document.

22. A method in accordance with the method of claim 20 wherein at least part of the partially encrypted document file is further encrypted to form a twice-encrypted file using a second encryption key, further comprising the step of prior to printing at least a second portion of said partially decrypted document file, decrypting said twice-encrypted file using at least said second encryption key.

23. A method in accordance with the method of claim 21 wherein said step of creating a serialized print number further comprises the step of generating, by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device.

CERTIFICATE OF TRANSMISSION
I hereby certify that this paper and every paper referred to therein as being facsimile transmitted to: (703) 872-9319 of the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on February 28, 2005 (Date of Deposit) No. of Pages 50

EDMOND A. DEFRANK
By

Signature

Attorney Docket No: 10001687-1 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of Kevin G. Currans	Group Art Unit: 2131
Entitled: **ASSURED PRINTING OF DOCUMENTS OF VALUE**	Examiner: C. Shin Hon
Serial No.: 09/641,929	
Filing Date: August 17, 2000	

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, LP.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to the assignee which will directly affect or be directly affected by or have a bearing on the Board's decision pending the appeal.

III. STATUS OF CLAIMS

Claim 5 has been cancelled and claims 1-4 and 6-23 stand rejected. Thus, the

Appellants file the present Appeal Brief in response to the Examiner's rejection of claims 1-4 and 6-23 in a Final Office Action dated September 2, 2004. Claims 1-4 and 6-23 represent all of the remaining claims from the originally filed application. The Appellants respectfully appeal the Examiner's final rejection of Claims 1-4 and 6-23.

IV. STATUS OF AMENDMENTS

An amendment under 37 CFR 1.116 was filed on November 2, 2004 in response to the Final Office Action dated September 2, 2004. In this amendment, minor non-substantive amendments were made to claims 1 and 4. In response, the Examiner sent an Advisory Action dated December 15, 2004 and checked the box on the Advisory Action form (PTOL-303) stating that the proposed amendment would not be entered, without providing any additional explanation. As such, claims 1-4 and 6-23 remain as presented in the May 27, 2004 amendment.

V. SUMMARY OF THE INVENTION

The present invention provides a method and apparatus for controlling printing of a document delivered via a computer network. In general, a first portion of a document is encrypted using at least a first encryption key, thereby creating a partially encrypted file. The partially encrypted file is transmitted via the computer network. A second portion of the transmitted partially encrypted file is printed and at least a serialized print number is returned. In response, the first encryption key is received. The first portion of the partially encrypted file is then decrypted and printed. This allows verification that the document was printed from an electronic file that was transmitted to and printed from a remote print mechanism and enables a document or file distributor to control re-distribution by conclusively determining whether a document printed from a file was printed in whole or in part.

In particular, the process includes the steps of encrypting a document and or parts thereof that is to be transferred electronically, transmitting the encrypted document to an intended party via a data network, such as the Internet, partially decrypting the document using a first decryption key so as to enable the document to be verified that it was properly received, and printing part of the document up to a point at which a second decryption key

is required. If the document is successfully printed down to the point where a second encryption key is required, the recipient of the document returns to the sender, an indicia, such a serial number of the document, which has been physically printed on the document at the time, that the document had started to print successfully. Receipt of the partial-printing proof by the document sender triggers the transmission to the document recipient (i.e., the printer and not the user's browser), the second decryption key by which the remaining portion of the document can be decrypted and printed by the recipient (i.e., the printer and not the user's browser).

Receipt of the indicia that the document was at least partially printed is created by the recipient's printer or print mechanism using a "Serialized Print." Upon the document sender's receipt of the indicia that the document was at least partially printed, the document recipient will thereby have provided to the document sender, conclusive proof that the entire document was received successfully as a "Guaranteed Print." The accuracy of the document that was printed can be determined and numerical indicia of output print quality can be generated such that a document sender provided with the print quality indicia can know whether the document that was printed was in fact a reasonably facsimile of the document that was electronically sent. Using the indicia of printing that was received by the sender, as well as an objective indicia of the output print quality documents that are sent electronically but which do not reasonable resemble their original condition as sent by the sender can be selectively retransmitted by the document sender at the document sender's discretion.

VI. ISSUES

Patentability of Claims 1-4 and 6-23

Whether claims 1, 2, 4, 6, 7, 10, 20, 21 and 23 are unpatentable under 35 U.S.C. § 103(a) over six (6) references including Christensen et al. (U.S. Publication No. US2002/0071559) in view of Nunley et al. (U.S. Patent No. 4,404,649) and further in view of Blumenthal et al. (U.S. Patent No. 5,784,460) and further in view of Wiegley (U.S. Patent No. 6,711,677) and further in view of Sansone (U.S. Patent No. 6,373,587) and further in view of Nishikawa (U.S. Pub. No. 20020048039).

Whether claims 3 and 22 are unpatentable under 35 U.S.C. § 103(a) over seven (7) references including Christensen et al. in view of Nunley et al. and further in view of Blumenthal et al. and further in view of Wiegley and further in view of Sansone and further in view of Nishikawa and further in view of Chan et al. (U.S. Patent No. 6,378,070).

Whether claims 12, 13, 17 and 18 are patentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg et al. (U.S. Patent No. 6,363,357) and further in view of Wiegley and further in view of Sansone and further in view of Nishikawa (U.S. Pub. No. 20020048039).

Whether claim 14 is unpatentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg and further in view of Sansone. Whether claim 16 is unpatentable under 35 U.S.C. § 103(a) over Christensen et al. in view of Rosenberg and further in view of Sansone and further in view of Blumenthal et al.

VII. GROUPING OF CLAIMS

For each ground of rejection which appellant contests herein which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

VIII. ARGUMENTS

A. The Examiner's Rationale for the Rejection of Claims 1-4 and 6-23

On pages 2 through 6 of the Final Office Action dated September 2, 2004, the Examiner discussed numerous references, one at a time in rejecting the claims. During the discussion of each reference, first the Examiner compared a single element of the Appellant's claims to a single element of a main cited reference. Second, the Examiner admitted that a second element of the Appellant's claims was not disclosed by the main reference but stated that it would have been obvious to add a second element of a second cited reference. Next, the Examiner admitted that the main and second references lacked a third element of the Appellant's claims but stated that it would have been obvious to add a third element of a third cited reference to the main and second references. The

Examiner then admitted that the third, second and main references lacked a fourth element of the Appellant's claims but stated that it would have been obvious to add a fourth element of a fourth cited reference to the main, second and third references. The Examiner then admitted that the fourth, third, second and main references lacked a fifth element of the Appellant's claims but stated that it would have been obvious to add a fifth element of a fifth cited reference to the main, second, third and fourth references. The Examiner then admitted that the fifth, fourth, third, second and main references lacked a sixth element of the Appellant's claims but stated that it would have been obvious to add a sixth element of a sixth cited reference to the main, second, third, fourth and fifth references.

With regard to claims 1, 2, 4, 6, 7, 10, 11, 20, 21 and 23, the Examiner continued this piece-meal approach of "tacking-on" another element of another reference each time an element of the claims was not disclosed, taught or suggested in the previous reference until **six (6)** references were combined. With regard to claims 3 and 22, the Examiner continued this "tacking-on" approach until **seven (7)** references were combined.

B. The Appellant Submits that the Examiner's Rejections Were Improper.

1. The Examiner ignored limitations of the claims and mischaracterized the references, thus, the rejections should be withdrawn.

According to case law and the MPEP, all of the claimed elements of an Appellant's invention **must be considered**. (In re Kotzab, 55 USPQ 2d 1313, 1318 (Fed. Cir. 2000). *MPEP 2143.*) [*emphasis added*]. If **one** of the elements of the Appellant's invention is missing from or not taught in the cited references and the Appellant's invention has advantages not appreciated by the cited references, then no prima facie case of obviousness exists. (*MPEP 2143.03).* The Federal Circuit Court has stated that it was error not to distinguish claims over a combination of prior art references where a material limitation in the claimed system and its purpose was not taught therein. In Re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

The cited combined references do **not** disclose, teach or suggest the Appellant's claimed invention that includes decrypting at the printer a first portion of the partially

encrypted file, printing at least a second portion of the partially encrypted file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and printing at least a portion of the decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

In contrast, although the Examiner used Nunley et al. as a reference to show serialized printing, the Examiner mischaracterized Nunley. Namely, Nunley does **not** disclose, teach or suggest the Appellant's serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

Instead, Nunley et al. uses a pre written SICN on the original document to support data entry and **not** a unique serialized print number for the document file in the course of printing the document file, like the Appellant's claimed invention. Nunley et al. is using the SICN merely to produce a customer reference for getting data entry information for the record in question. Consequently, the Examiner mischaracterized Nunley et al., and thus, obviousness cannot be established by combining these references because Nunley et al. is missing elements of the Appellant's claim. ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). This **failure** of the combined cited references to disclose, suggest or teach all of the elements of the Appellant's claimed invention indicates a lack of a prima facie case of obviousness (*MPEP 2143*).

2. The Examiner ignored a teaching away, thus, the rejections should be withdrawn

Even though the combination of the **six or seven** cited references **does not** produce all of the elements of the claimed invention, these references **should not** even be considered together since there is no motivation to combine the cited references. It is well-

settled law that there **must be** a basis in the references for combining or modifying the references. C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 48 USPQ 2d 1225, (Fed. Cir. 1998).

Specifically, obviousness cannot be established because Christensen et al. **teaches away** from the claimed invention. This is because the computer in Christensen et al. first fully decrypts the document and then transmits the fully decrypted document to the printer, which teaches away from the Appellant's claimed performing decryption at the printer. In particular, Christensen et al. explicitly states in the Abstract that encrypted "...data is transmitted from a first computer to a second computer, and the decryption key has to be requested each time the user want to gain access to the data in an unencrypted form." Moreover, Christensen et al. continues to state in parapgraph [0022] that "...(i.e. after K.sub.d has been used to decrypt the encrypted data) K.sub.d must be rendered unfit for use. This must be done in order to prevent the user from gaining access to K.sub.d. That is, K.sub.d may only be obtained and used temporarily, and the user may not at any time gain direct access to K.sub.d."

As a result, modifying the decryption location in Christensen et al. would modify the entire system in Christensen et al. and render the system being modified unsatisfactory for its intended purpose. Hence, the main function of Christensen et al. would be destroyed because the system in Christensen et al. specifically requires decryption at the computer. For example, if decryption were moved, an unscrupulous user would be able to modify the printer driver, for example, by changing the printer driver name. In this case, the unscrupulous user would be able to electronically capture the print job and redistribute it easily. In many cases, printer drivers are represented and differentiated by their device context, which is stored in the registry, and can easily be shared via a registry file.

As required by the case law and the MPEP, "[I]f proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). MPEP 2143.01. Therefore, the proposed modification is **not** proper and one of ordinary skill in the art would not find a reason to make the proposed modification. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

As such, this "teaching away" cannot be ignored. As such, obviousness cannot be established by combining these references. W.L. Gore& Assocs. V. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983).

3. The Examiner used improper hindsight to reject the claims, thus, the rejections should be withdrawn.

It is well-settled law that there must be a basis in the references for combining or modifying the references. Namely, the Examiner **cannot** use a "tack-on" approach to **arbitrarily "pick and choose" elements** from numerous references and combine these elements using hindsight. Any combination of elements in a manner that reconstructs the Appellant's invention only with the benefit of **hindsight** is insufficient to present a prima facie case of obviousness. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 230 USPQ 416 (Fed. Cir. 1986). [*emphasis added*].

Evidence that the Examiner used hindsight is clearly confirmed by the fact that the Examiner cited six (6) references for a single rejection and seven (7) references for another single rejection without providing any reasoning for combining these references. Contrary to the Examiner's approach, the Appellant submits that there must be some reason, suggestion, or motivation found in the references whereby a person of ordinary skill in the field of the invention would make the combination. **That knowledge cannot come from the applicant's invention itself.** In re Oetiker, 977 F.2d 1443, 24 USPQ 2d 1443, 1446 (Fed. Cir. 1992) [*emphasis added*].

Further, "[T]he genius of invention is often a combination of known elements which in hindsight seems preordained. To prevent hindsight invalidation of patent claims, the law requires some 'teaching, suggestion or reason' to combine cited references." Gambro Lundia AB v. Baxter Healthcare Corp., 110 F.3d 1573, 1579, 42 USPQ 2d 1378, 1383 (Fed. Cir. 1997). When the reference in question seems relatively similar "...**the opportunity to judge by hindsight is particularly tempting**. Consequently, the tests of whether to combine references need to be applied rigorously," especially when the Examiner uses numerous references. McGinley v. Franklin Sports Inc., 60 USPQ 2d 1001, 1008 (Fed. Cir. 2001). [*emphasis added*]. Since the Examiner's rejection is

unquestionably based on hindsight, the rejection is improper and must be withdrawn. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.

IX. CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-4 and 6-23 was erroneous, and reversal of the Examiner's decision is respectfully requested. Accordingly, the Appellants submit that all pending claims (claims 1-4 and 6-23) in the current case should be allowed.

Respectfully submitted,

Dated: February 28, 2005

Edmond A. DeFrank
Reg. No. 37,814
Attorney for Appellants

EDMOND A. DEFRANK
Attorney at Law
20145 Via Medici
Northridge, CA 91326
(818) 885-1575 TEL
(818) 885-5750 FAX

X. APPEAL BRIEF APPENDIX

The following represents claims 1-4 and 6-23 that are involved in the appeal of the above-identified application and are provided in accordance with the requirements of 37 CFR 1.192(c)(7). Claim 5 is not presented below because it was cancelled in a May 27, 2004 amendment:

1. A method to control printing of a document file delivered via a computer network comprising the steps of:

at a first computer:

encrypting at least a first portion of a document file using at least a first encryption key thereby creating a partially encrypted file;

transmitting the partially encrypted file to a second computer via said computer network;

at said second computer:

printing at least a second portion of said partially encrypted file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file;

returning to said first computer at least the serialized print number, and receiving, in response thereto, said first encryption key;

decrypting at the printer said first portion of said partially encrypted file to create a partially decrypted document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

2. A method in accordance with the method of claim 1 wherein said step of returning further comprises the step of providing payment.

3. A method in accordance with the method of claim 1 further including steps of:

before transmitting the partially encrypted file to a second computer, encrypting at least part of said partially encrypted file to form a twice-encrypted file using a second encryption key; and

prior to printing at least a second portion of said partially decrypted file, decrypting said twice-encrypted file using at least one of either said second encryption key or a third encryption key.

4. A method in accordance with the method of claim 1 wherein said serialized print methodology includes the steps of:

generating by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device;

returning said number to said first computer thereby enabling said second computer to receive said first key.

5. (canceled).

6. A system for controlling the printing of a document file delivered via a computer network comprising:

a first computer that encrypts at least a first portion of a document file using a first key;

a data transfer device coupled said first computer capable of transferring the partially encrypted document file to a second computer;

a print mechanism operatively coupled to said data transfer device, said print mechanism capable of receiving said document file and decrypting at least a portion of said first portion of said document file and printing said first portion using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

7. The system of claim 6 wherein said print mechanism is comprised of a computer operatively coupled to a printer.

8. The system of claim 6 wherein said print mechanism is comprised of a printer capable of generating serialized output.

9. The system of claim 6 wherein said print mechanism is comprised of a printer capable of guaranteeing output print quality.

10. Apparatus for controlling the printing of a document file delivered via a computer network, comprising:

a first computer coupled to a data transfer mechanism, said first computer capable of receiving via said data transfer mechanism, at least one partially encrypted document file from a second computer;

a print mechanism operatively coupled to said first computer, said print mechanism being capable of decrypting at least a portion of the encrypted file and printing at least a portion of said partially encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

11. Apparatus for controlling the printing of a document file delivered via a computer network comprising:

a first computer coupled to an Internet connection, said first computer capable of receiving data from a remote printer via said Internet connection, at least one partially encrypted document file from a second computer;

a networked print mechanism operatively coupled to said first computer via the Internet, said print mechanism being capable of decrypting at least a portion of the encrypted file and printing at least a portion of said partially encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said partially decrypted document file using a guaranteed print methodology that includes sending via the Internet the first computer information about the number of printed pages and output print quality of the document file.

12. A method of controlling the printing of a document delivered via a computer network comprising the steps of:

printing a first portion of the document with a remote printer, said first portion being unencrypted;

communicating, via the computer network, with an entity associated with the document to arrange for the printing of a remaining portion of the document;

receiving, as a result of said communicating step, an encrypted remaining portion of the document;

using the printer to decrypt said remaining portion;

printing said decrypted remaining portion using a guaranteed print methodology that includes sending information about the number of printed pages and output print quality of the document file; and

using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file.

13. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of providing payment to said entity.

14. A method in accordance with the method of claim 12 wherein said communicating step further comprises the step of ascertaining quality of said printed first portion.

15. A method in accordance with the method of claim 12 further comprises the step of generating a number correlating said document to a printing device printing said first portion.

16. A method in accordance with the method of claim 15 wherein said step of communicating further comprises the step of communicating said generated number.

17. A method of controlling the printing of a document delivered via a computer network to a user, comprising of the steps of:

encrypting a portion of the document;

transmitting an unencrypted portion of the document via the computer network to the user for printing;

receiving a communication related to a reception of said unencrypted portion by the user;

transmitting said encrypted portion of the document to the user via the computer network in response to said receiving step;

using a printer to decrypt at least a portion of the encrypted file and printing at least a portion of said encrypted document file using a serialized print methodology that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file; and

printing at least a portion of said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

18. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a payment for the document.

19. A method in accordance with the method of claim 17 wherein said receiving step further comprises the step of receiving a proof that said unencrypted portion of the document was satisfactorily printed.

20. A method of controlling the printing of a partially encrypted document file delivered via a computer network, at least a first portion of which partially encrypted document is encrypted using at least a first encryption key, comprising the steps of:

printing using a printer at least a second portion of the partially encrypted document file;

creating a serialized print number that includes having the printer generate a unique serialized print number for the document file in the course of printing the document file and returning the serialized print number via the computer network;

receiving the first encryption key;

using the printer to decrypt the first portion to create a decrypted document file; and

printing said decrypted document file using a guaranteed print methodology that includes sending the first computer information about the number of printed pages and output print quality of the document file.

21. A method in accordance with the method of claim 20 further comprising the step of providing payment for the partially encrypted document.

22. A method in accordance with the method of claim 20 wherein at least part of the partially encrypted document file is further encrypted to form a twice-encrypted file using a second encryption key, further comprising the step of prior to printing at least a second portion of said partially decrypted document file, decrypting said twice-encrypted file using at least said second encryption key.

23. A method in accordance with the method of claim 21 wherein said step of creating a serialized print number further comprises the step of generating, by a device printing said decrypted document file, a number correlating said decrypted document file to said printing device.